Original-URL des Artikels: https://www.golem.de/news/governikus-personalausweis-webanwendungen-lassen-sich-austricksen-1811-137831.html **Veröffentlicht:** 21.11.2018 11:12
Kurz-URL: https://glm.io/137831

Governikus

Personalausweis-Webanwendungen lassen sich austricksen

Mit einem relativ simplen Trick lässt sich die Authentifizierung von Webanwendungen mit dem elektronischen Personalausweis austricksen. Der Hersteller Governikus behauptet, dass dies in realen Anwendungen nicht funktioniert, kann aber nicht erklären, warum.

Die Firma SEC Consult hat in einer Bibliothek für den elektronischen Personalausweis eine Sicherheitslücke gefunden. Das sogenannte Autent SDK der Firma Governikus erlaubt es, die Signaturprüfung auszutricksen.

Der elektronische Personalausweis in Deutschland erlaubt es Nutzern, mittels eines darauf vorhandenen RFID-Chips sich gegenüber Webanwendungen zu authentifizieren. Dafür benötigt der Nutzer einen passenden Kartenleser und eine Client-Software.

Signaturprüfung bei der einen, Datenauswertung bei der anderen Variablen

Die Software kommuniziert dabei mit einem vertrauenswürdigen Authentifizierungsserver, der anschließend eine entsprechende Anfrage signiert. Diese signierte Anfrage im SAML-Format wird anschließend an die jeweilige Webanwendung, die die Personalausweisfunktion nutzt, weitergeleitet und von dieser geprüft. Für solche Webanwendungen stellt die Firma Governikus eine in Java geschriebene Bibliothek bereit, das sogenannte Autent SDK.

<#youtube id="kaATyYmpiIE"> Die Anfragen, die an die Webanwendung weitergeleitet werden, sind in der URL in einer GET-Variablen namens SAMLResponse codiert. Das Problem: Man kann diese Variable auch mehrfach in der URL angeben. Die Autent-Software prüft dann die Signatur der letzten in der URL übergebenen Variablen. Verarbeitet werden aber die Daten aus der ersten übergebenen Variablen.

Das Ergebnis: Ein Angreifer kann eine beliebige, gültig signierte SAML-Anfrage verwenden und gleichzeitig eine nicht gültig signierte andere SAML-Anfrage mitschicken - und sich so beispielsweise als jemand anderes ausgeben. Es wird dabei auch nicht geprüft, ob die Anfrage vom richtigen Nutzer stammt.

Ein Angreifer kann sich also selbst vom Authentifizierungsserver eine gültige Signatur für irgendeine Anfrage geben lassen und dann im Namen einer anderen Person eine Aktion durchführen.

Unerklärbare Sicherheitsmaßnahmen verhindern angeblich Angriff

Auf Anfrage teilte Governikus mit, dass der Angriff von SEC Consult nur in einer Beispielanwendung durchgeführt wurde. *"Veröffentlicht wurde dieses Demo-Beispiel im Rahmen eines Anwenderforums, um aufzuzeigen, wie schnell die Online-Ausweisfunktion integriert werden*

kann", schreibt Governikus dazu. *"Kein uns bekanntes, reales Einsatzszenario basiert auf diesem Demo-Beispiel bzw. wurde die Integration ohne weitere Sicherheitsmaßnahmen durchgeführt."*

Auf nochmalige Nachfrage hin behauptete Governikus auch, dass diese zusätzlichen Sicherheitsmaßnahmen den Angriff verhindern würden. Eine Erklärung, wie dies geschieht, bekamen wir jedoch trotz mehrfacher Nachfrage nicht. Governikus verwies lediglich auf zwei längere Dokumente zur Sicherheit von SAML-Anwendungen und schrieb uns, dass Governikus seinen Kunden empfiehlt, die dortigen Maßnahmen umzusetzen. Inwiefern diese den Angriff verhindern, konnte Governikus uns jedoch trotz mehrerer Rückfragen nicht erklären.

Was macht die Personalausweis-Bibliothek im beA?

SEC Consult weist in einem uns vorab zur Verfügung gestellten Dokument darauf hin, dass das Autent SDK auch Teil der Software für das besondere elektronische Anwaltspostfach (beA) ist. Wir konnten das nachvollziehen, es ist aber unklar, welche Rolle es dort spielt. Eine Online-Authentifzierungsfunktion mit dem Personalausweis ist im beA nicht vorgesehen. Die Bundesrechtsanwaltskammer hat eine entsprechende Anfrage bisher nicht beantwortet.

Die Firma SEC Consult selbst hat 2015 einen Sicherheitstest des beA durchgeführt, das neben dem Autent SDK noch zahlreiche andere Komponenten von Governikus enthält.

Zu den Ergebnissen dieses Sicherheitstests schweigen alle Beteiligten bis heute. Es ist völlig unklar, wie die zahlreichen teilweise sehr trivialen Sicherheitslücken, die im BeA gefunden wurden, bei diesem Sicherheitstest von SEC Consult übersehen wurden. Entsprechende Anfragen an die Bundesrechtsanwaltskammer nach dem Informationsfreiheitsgesetz wurden alle abgelehnt. SEC Consult teilt auf Anfrage mit, dass es Fragen dazu nicht kommentieren kann.

Elektronischer Personalausweis kein Erfolgsprojekt

Den Personalausweis mit Chipkarte gibt es in Deutschland seit 2010. Ein großer Erfolg ist er bislang nicht. Immer wieder wird gemeldet, dass die Onlinefunktion kaum genutzt wird und dass es nur wenige Dinge gibt, die man überhaupt mit dem Personalausweis Online erledigen kann. Wegen Sicherheitslücken waren der Personalausweis und die zugehörige Software vor längerer Zeit schon öfter in den Schlagzeilen. (hab)

Verwandte Artikel:
Terrorismus: EU-Kommission will Fingerabdrücke in allen Personalausweisen
(16.04.2018, https://glm.io/133855)
Der Bund und die Cloud: "Bürgerdaten sind ein Schatz"
(27.04.2012, https://glm.io/91465)
Gerichtspostfach: EGVP-Client kann weiter genutzt werden
(21.01.2018, https://glm.io/132277)
Ende-zu-Ende-Verschlüsselung: Klage gegen Anwaltspostfach eingereicht
(18.06.2018, https://glm.io/134984)
BSI-Richtlinie: CCC und OpenWRT kritisieren Router-TR als "Farce"
(19.11.2018, https://glm.io/137796)
